The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2010

SUBJECT:
Vulnerability in Microsoft MPEG Layer-3 Codec Could Allow Remote Code Execution (MS10-052)

OVERVIEW:
A vulnerability has been discovered in the Microsoft MPEG Layer-3 Codec for Microsoft DirectShow that could allow an attacker to take complete control of a vulnerable system. A codec is software that is used to compress or decompress digital media content, such as a song or video. This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Windows XP SP3
Windows Server 2003

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Microsoft MPEG Layer-3 Audio Codec for Microsoft DirectShow which could allow an attacker to take complete control of an affected system. The vulnerability affects the Microsoft MPEG Layer-3 Audio Codec for Microsoft DirectShow 'l3codecx.ax' file specifically. Microsoft DirectShow technology performs client-side audio and video sourcing, manipulation and rendering. Specifically, this issue arises because the Microsoft MPEG Layer-3 codec for Microsoft DirectShow does not perform sufficient boundary checks when processing maliciously crafted MPEG Layer-3 content through the Microsoft DirectShow API. This results in a heap-based buffer overflow condition that could allow for remote code execution if successful. MPEG Layer-3 content could be included in audio and video files, streaming content from web pages, or other rich media content capable file formats (PowerPoint slides, Word documents, Adobe Flash content, and many others).

This vulnerability can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted media file as an email attachment. In the Web based scenario, a user would have to open a specially crafted media file that is hosted on a website. Successful exploitation could result in an attacker gaining the same privileges as the logged on user.

Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS10-052.mspx

Secunia:
http://secunia.com/advisories/40934

Security Focus:
http://www.securityfocus.com/bid/42298
http://www.securityfocus.com/archive/1/512981

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1882